Automating Scans in Your CI/CD Pipeline

Neil Morrissey
SOLUTIONS ARCHITECT

@morrisseycode www.neilmorrissey.net

Module Overview

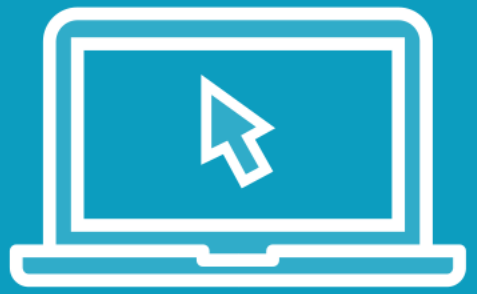
Configuring SonarCloud in a build pipeline

Scanning open-source libraries using WhiteSource Bolt

Configuring OWASP Zap in a release pipeline

Configuring SonarCloud in a Build Pipeline

Demo



- Create SonarCloud account
- Generate SonarCloud security token
- Create SonarCloud project
- Add SonarCloud extension to Azure DevOps organization
- Configure service connection to SonarCloud
- Add SonarCloud tasks to build pipeline
- Run build and view analysis results in SonarCloud

Configuring OWASP Zap in a Release Pipeline

Demo

- Create a Release Pipeline
- Install Docker CLI
- Pull and Run OWASP Zap Container
- Transform Report to NUnit Format
- Save Generated Reports
- Publish Test Report to Release Pipeline

Course Summary

AZ-400 exam objectives: developing security and compliance

Static and dynamic application security testing

Dependency scanning

Secrets scanning

Configuration of common tooling

Thank You, and Good Luck!

Neil Morrissey

@morrisseycode www.neilmorrissey.net